

THE PORT AUTHORITY OF NY & NJ

Law Department

*4 World Trade Center
150 Greenwich Street
New York, NY 10007*

July 15, 2019

Ms. Emma Best
MuckRock News
DEPT MR 75722
411 A Highland Ave
Somerville, MA 021442516
Email: 75722-68239710@requests.muckrock.com

Re: Public Records Access No. 20555

Dear Ms. Best:

This is in response to your June 21, 2019 request, which has been assigned the above-referenced filing number under the Port Authority's Public Records Access Policy.

We would be very happy to respond to your request. But as it is currently framed, your request is exceptionally broad. The request is not specific and precise as to what records are actually being sought, and the request seeks an inordinately large volume of records. Broad requests can require an enormous expenditure of agency resources and can take an especially long period of time for us to turn around on your behalf. And with broad requests, it can be especially difficult for us to discern what is important to the requester, and what the requester may have included only to help ensure that he or she is getting what is especially crucial from his or her perspective. Against this backdrop, we ask that you modify your request, to make it substantially more narrow and more specific --- so that we can work efficiently, with a focus on getting you the materials that are most important to you. If we don't hear from you one way or another within five business days, we will close this request. If we do hear from you within five business days, we will begin our work.

Please identify the records being requested and the time frame.

Very truly yours,



Bin Bin Chen
FOI Administrator

From: 75722-68239710@requests.muckrock.com
Sent: Friday, June 21, 2019 1:13 PM
To: PA FOI
Subject: New York Freedom of Information Law Request: Criminal Hackers Target Police to Protest Perceived Injustices (The Port Authority of New York and New Jersey)
Attachments: DHS-FBI-HackersTargetPolice.pdf

CAUTION: This email originated from outside the Port Authority. Do not open attachments or click on links from unknown senders or unexpected emails.

The Port Authority of New York and New Jersey
FOIL Office
4 World Trade Center, 25th Floor
150 Greenwich Street
New York, NY, NY 10007

June 21, 2019

To Whom It May Concern:

Pursuant to the New York Freedom of Information Law, I hereby request the following records:

Records mentioning, describing or generated as a result of the 8 May 2015 Roll Call Release IA-0181-15 (which was designed to be shared widely with law enforcement) from the Department of Homeland Security's Office of intelligence and Analysis (I&A) in conjunction with the Federal Bureau of Investigation, titled "Criminal Hackers Target Police to Protest Perceived Injustices," as well as records otherwise responding or reacting to the issues raised in it.

I am a member of the news media and request classification as such. I have previously written about the government and its activities, with some reaching over 100,000 readers in outlets such as Gizmodo, MuckRock, Motherboard, Property of the People, Unicorn Riot, and The Outline, among others. As such, as I have a reasonable expectation of publication and my editorial and writing skills are well established. In addition, I discuss and comment on the files online and make them available through non-profits such as the library Internet Archive and the journalist non-profit MuckRock, disseminating them to a large audience. While my research is not limited to this, a great deal of it, including this, focuses on the activities and attitudes of the government itself.

As my primary purpose is to inform about government activities by reporting on it and making the raw data available, I request that fees be waived.

The requested documents will be made available to the general public, and this request is not being made for commercial purposes.

In the event that there are fees, I would be grateful if you would inform me of the total charges in advance of fulfilling my request. I would prefer the request filled electronically, by e-mail attachment if available or CD-ROM if not.

Thank you in advance for your anticipated cooperation in this matter. I look forward to receiving your response to this request within 5 business days, as the statute requires.

Sincerely,

Emma Best

Filed via MuckRock.com

E-mail (Preferred): 75722-68239710@requests.muckrock.com

Upload documents directly:

[https://accounts.muckrock.com/accounts/login/?url_auth_token=AAATjr4IXB07AWpztaqiXXvHfxY%3A1heN5x%3AAP-](https://accounts.muckrock.com/accounts/login/?url_auth_token=AAATjr4IXB07AWpztaqiXXvHfxY%3A1heN5x%3AAP-1FydCP88yYFHRhpLGzAABgjs&next=https%3A%2F%2Fwww.muckrock.com%2Faccounts%2Flogin%2F%3Fnext%3D%252Faccounts%252Fagency_login%252Fthe-port-authority-of-new-york-and-new-jersey-2408%252Fcriminal-hackers-target-police-to-protest-perceived-injustices-the-port-authority-of-new-york-and-new-jersey-75722%252F%253Femail%253Dpafoi%252540panynj.gov)

[1FydCP88yYFHRhpLGzAABgjs&next=https%3A%2F%2Fwww.muckrock.com%2Faccounts%2Flogin%2F%3Fnext%3D%252Faccounts%252Fagency_login%252Fthe-port-authority-of-new-york-and-new-jersey-2408%252Fcriminal-hackers-target-police-to-protest-perceived-injustices-the-port-authority-of-new-york-and-new-jersey-75722%252F%253Femail%253Dpafoi%252540panynj.gov](https://accounts.muckrock.com/accounts/login/?url_auth_token=AAATjr4IXB07AWpztaqiXXvHfxY%3A1heN5x%3AAP-1FydCP88yYFHRhpLGzAABgjs&next=https%3A%2F%2Fwww.muckrock.com%2Faccounts%2Flogin%2F%3Fnext%3D%252Faccounts%252Fagency_login%252Fthe-port-authority-of-new-york-and-new-jersey-2408%252Fcriminal-hackers-target-police-to-protest-perceived-injustices-the-port-authority-of-new-york-and-new-jersey-75722%252F%253Femail%253Dpafoi%252540panynj.gov)

Is this email coming to the wrong contact? Something else wrong? Use the above link to let us know.

For mailed responses, please address (see note):

MuckRock News

DEPT MR 75722

411A Highland Ave

Somerville, MA 02144-2516

PLEASE NOTE: This request is not filed by a MuckRock staff member, but is being sent through MuckRock by the above in order to better track, share, and manage public records requests. Also note that improperly addressed (i.e., with the requester's name rather than "MuckRock News" and the department number) requests might be returned as undeliverable.



ROLL CALL RELEASE

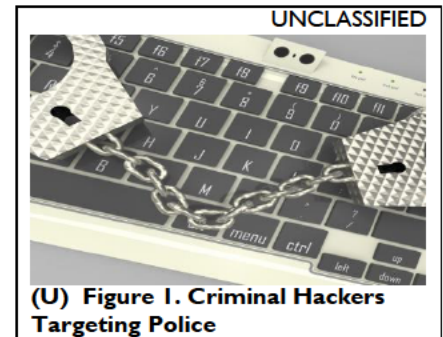
INTELLIGENCE FOR POLICE, FIRE, EMS, AND SECURITY PERSONNEL

8 May 2015

(U//FOUO) Criminal Hackers Target Police to Protest Perceived Injustices

(U//FOUO) Disruptive cyber attacks by criminal hackers—primarily distributed-denial-of-service (DDoS) attacks—targeting local law enforcement websites have increased since August 2014. We judge that this is almost certainly a result of the heightened coverage surrounding the alleged use of excessive force by law enforcement and an increased focus on incidents of perceived police brutality. The primary impact from the majority of these attacks has been the temporary disruption of the targeted public-facing websites.

- » (U//FOUO) In 2014, the Multi-State Information Sharing and Analysis Center (MS-ISAC) observed 53 separate incidents of criminal hackers conducting cyber operations against state and local entities in response to incidents of alleged use of excessive force by law enforcement. The majority of these incidents were low to moderate in effect, most frequently resulting in temporary disruption to targeted websites.
- » (U//FOUO) On the morning of 30 December 2014, unknown criminal hackers disabled a Midwestern police department's public website using a DDoS attack. A post later that morning on a US social-networking site containing the hashtag "#BlackLives Matter" announced that the targeted website was down. The disabling of this website was the third successful attack to disable a law enforcement website in the state within a week—the attacks were limited to the temporary disablement of targeted websites, according to DHS field reporting.
- » (U//FOUO) A criminal hacker using the moniker (at)DigitaShadow claimed responsibility on a US social-media site for disrupting access to a Northwestern city police department's website in early December 2014. The DDoS attack, which lasted approximately 10 minutes, prevented the department's in-car terminals from transmitting or receiving traffic, including 911 dispatch requests, according to FBI reporting.



(U) Figure 1. Criminal Hackers Targeting Police

(U//FOUO) MS-ISAC Distributed-Denial-of-Service Mitigation Recommendations

(U) Proactive protections include:

- » (U) Establish connections with multiple Internet service providers (ISPs) for redundancy,
- » (U) Ensure service-level agreements with ISPs contain provisions for DoS prevention (such as IP address rotation),
- » (U) Conduct rate-limiting of traffic at the network perimeter, and
- » (U) Create backup, remote-site network infrastructure using multiple addressing schemes.

(U) Reactive protections include:

- » (U) Execute ISP address rotation,
- » (U) Block source IP addresses generating DoS traffic at enterprise boundary or within ISP infrastructure, and
- » (U) Acquire increased bandwidth capability from the ISP.

(U//FOUO) See MS-ISAC's "Guide to DDoS Attacks" for additional information:

http://msisac.cisecurity.org/resources/reports/documents/GuidetoDDoSAttacks_000.pdf.

(U) Reporting Computer Security Incidents

(U) To report a computer security incident, either contact US-CERT at 888-282-0870, or go to <https://forms.us-cert.gov/report/> and complete the US-CERT Incident Reporting System form. The US-CERT Incident Reporting System provides a secure, web-enabled means of reporting computer security incidents to US-CERT. An incident is defined as a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard computer security practices. In general, types of activity commonly recognized as violating typical security policies include attempts (either failed or successful) to gain unauthorized access to a system or its data, including personally identifiable information; unwanted disruption or denial of service; the unauthorized use of a system for processing or storing data; and changes to system hardware, firmware, or software without the owner's knowledge, instruction, or consent.

IA-0181-15

(U) Prepared by the Office of Intelligence and Analysis (I&A). Coordinated with the FBI. This product is intended to provide cybersecurity awareness to federal, state, local, and private sector first responders in matters that can affect personnel and network security of their respective organizations.

(U) **Warning:** This document is UNCLASSIFIED//FOR OFFICIAL USE ONLY (U//FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information and is not to be released to the public, the media, or other personnel who do not have a valid need to know without prior approval of an authorized DHS official. State and local homeland security officials may share this document with authorized critical infrastructure and key resource personnel and private sector security officials without further approval from DHS.